January 19, 2007

Federal Trade Commission
Office of the Secretary
Room H-135 (Annex N)
600 Pennsylvania Avenue, N.W.
Washington, DC 20850

RE: Identity Theft Task Force, P065410

Dear Sir or Madam:

America's Community Bankers (ACB)[1] is pleased to provide comments to the President's Identity Theft Task Force (Task Force). Identity theft is a serious threat to the United States in general and to financial institutions in particular. As custodians of sensitive customer information, financial institutions take the responsibility to protect that data very seriously. In addition, banks are unique in the United States' economy in that they are already subject to detailed requirements regarding data security that do not apply to other businesses.

ACB applauds the progress the Task Force has made to create a strategic plan to assist the federal government in battling identity theft. The progress is especially impressive since the Task Force was established by Executive Order less than one year ago in May 2006.

This submission is made in response to the Task Force announcement on December 26, 2006, seeking public comment on ways to reduce identity theft. The announcement asked for comment on several areas of interest related to the issue. ACB provides the comments below on those topics included in the announcement that we consider most critical for community banks.

[1] America's Community Bankers is the national trade association committed to shaping the future of banking by being the innovative industry leader strengthening the competitive position of community banks. To learn more about ACB, visit www.AmericasCommunityBankers.com.

900 Nineteenth Street, NW, Suite 400, Washington, DC 20006
Phone: (202) 857-3100 ★ Fax: (202) 296-8716 ★ www.AmericasCommunityBankers.com

ACB Recommendations

Comprehensive Record on Private Sector Use of Social Security Numbers (SSNs)

Financial institutions use SSNs to identify individuals, open accounts, and perform credit checks prior to granting loans, and therefore, use of SSNs is critical to the banking industry. We urge the Task Force to take into account any disruptions to the economy that might occur if use of SSNs were unduly restricted without an appropriate alternative being provided. Banks recognize the importance of protecting private information while simultaneously using it in the normal course of business. Indeed, the banking industry is subject to data security requirements imposed by Congress and the Federal banking agencies that do not apply to other businesses.

We support the Task Force's evaluation of the different ways private businesses use SSNs. If the Task Force decides to proceed with such an analysis, ACB would be pleased to provide an overview of how SSNs are used by banks and how such information is protected under banking regulations.

National Data Security Standards

ACB strongly supports a national standard for financial institutions maintaining sensitive customer information. A national standard would ensure that all consumers would have equal protection and allow businesses to focus on compliance with a single set of requirements. The growing patchwork of state laws and regulations increases the burden on entities maintaining the information, hurts the economy, and will not provide the most effective consumer protection.

ACB believes that the Task Force should recognize that the Gramm-Leach-Bliley Act (GLBA) already requires financial services companies to have in place much of the protections proposed over the years in other data security legislation. Title V of GLBA requires financial services companies to implement data security safeguards, a customer response program, and a comprehensive privacy policy. The banking regulators have issued guidance extending Title V to require customer notices in case of a breach that puts consumers at risk. Adding another layer of regulations to the existing requirements would be costly to the banks and, ultimately, to their customers.

ACB suggests that the robust data security framework that already exists at financial institutions could be a starting template for a national data security standard. Other businesses that hold sensitive information should be required to comply with standards similar to those currently imposed on financial institutions. Adding any additional layer of regulations to those already applicable to banks would be burdensome for banks and would not achieve the goal of better consumer protection. Finally, ACB believes that functional regulation is the best way to enforce data security standards. Any national standard applicable to banks should be enforced by the banking agency regulators that oversee them already.

Breach Notice Requirements for Private Sector Entities Handling Sensitive Consumer Information

ACB supports a national standard for providing notice to customers when the integrity of sensitive customer information has been compromised and poses a risk to consumers. The entity that is responsible for the breach must be clearly identified to the consumer and bear the costs of notifying the customer, even if it is not the one sending the notice. Breaches caused by third parties involving credit cards subject banks that issued the cards to significant reputation risk, even when the bank is not responsible for the breach. In addition, ACB believes that the entity that is responsible for a data breach should bear the costs of protecting consumers, including reimbursing the banks the cost of cancelling and reissuing credit or debit cards, as well as fraudulent charges to credit or debit cards. Currently those costs are being borne by the financial institution, even though it bears no responsibility for the breach. For example, the recent TJX Companies breech involves upwards of millions of credit and debit cards and numerous institutions. Yet the cost of re-issuance of these cards and the notification of the customers falls to the issuing institutions not to TJX Companies.

The banking regulators have issued guidance extending the Title V requirements of the GLBA to require customer notices in case of a breach that puts consumers at risk. ACB supports leaving this existing standard in place and extending the standard to non-bank businesses.

Education of the Private Sector and Consumers on Safeguarding Data

ACB supports a campaign to raise the awareness of individuals and businesses of the threat of identity theft. The campaign focusing on individuals should address how they should protect themselves using low-tech and high-tech methods. For example, the campaign should discuss the importance of shredding confidential paper documents, not disclosing sensitive information to strangers of the phone, increasing awareness of phishing emails and other cyber scams, and ensuring that personal computers are free of viruses. The campaign aimed at businesses would be dependent on the specifics of a national data security requirement and should detail their obligations to protect sensitive data, provide recommendations on how to protect that data, and set forth the consequences of failing to do so.

Making Identity Theft Victims Whole

ACB supports the Task Force recommendation that identity theft victims be allowed to seek restitution from identity thieves for the value of their time in attempting to recover from the crime.

However, it is not only the individual victims of identity theft that incur costs. For example, ACB members who must re-issue debit and credit cards when there are data breaches at third parties are also victims. The costs associated with card re-issuance are high and the banks should be reimbursed by those responsible for the breach.

Gathering Information on the Effectiveness of Victim Recovery Measures

ACB supports the Task Force's intent to study the amendments to the Fair and Accurate Transactions Act of 2003 (FACT Act) and the effectiveness of state credit freeze laws. Safeguards such as fraud alerts already exist under the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) In addition, although well-intentioned, state credit freeze laws may create a patchwork of requirements that are not uniform and that may significantly disrupt the highly efficient system of credit granting that has evolved in the United States. Allowing people to freeze their credit as a preemptive form of self-protection will result in many people being unable to gain access to credit when they most need it.

Ability of Law Enforcement to Receive Information from Financial Institutions

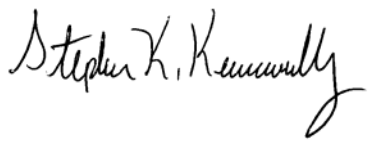
ACB supports enhanced communications with all federal entities in an effort to reduce identity theft. This position is supportive of the three initiatives cited in this section including the Justice Department/private sector promotion of Section 609(e) of the FCRA enabling identity theft victims to receive theft related documents and designate law enforcement agencies to receive them on their behalf, the federal law enforcement/private sector efforts to reduce mail fraud, and Justice Department/credit reporting agency discussions on reducing the risk associated with thieves accessing credit reports.

Targeted Enforcement Initiatives

ACB believes that the federal banking agencies are continuously reviewing the threat posed by identity theft. For example, the agencies recently released additional guidance requiring banks to assess their online banking security and to facilitate additional authentication security for their customers. This guidance was issued to prevent the misuse of customer funds by illegally obtaining a user name and password for an online account. The banking agencies recognized the growing threat of account hijacking and instituted a higher level of security. This is just one example of the standards applicable to banks that could be used as a model for other businesses.

ACB appreciates the opportunity to comment on this matter and supports the Task Force in its ongoing efforts against identity theft. Please contact the undersigned at 202-857-3148 or via email at skenneally@acbankers.org or Patricia Milon at 202-857-3121 if you have any questions.

Sincerely,



Stephen K. Kenneally
Director, Payments and Technology Policy